DEFENDANT TECHNICOLOR SA'S REPLY BRIEF IN SUPPORT OF ITS MOTION TO DISMISS FOR LACK OF PERSONAL JURISDICTION, IMPROPER VENUE, AND INSUFFICIENT SERVICE OF PROCESS

EXHIBIT 2

Declaration of Eric Diehl

IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
TYLER DIVISION

BLUE SPIKE, LLC Plaintiff, vs. TECHNICOLOR USA, INC. and TECHNICOLOR SA, Defendants.	)	Case No. 6:12-CV-00572 LED **JURY TRIAL DEMANDED**

DECLARATION OF ERIC DIEHL IN SUPPORT OF TECHNICOLOR SA'S REPLY BRIEF IN SUPPORT OF ITS MOTION TO DISMISS FOR LACK OF PERSONAL JURISDICTION, IMPROPER VENUE, AND INSUFFICIENT SERVICE OF PROCESS

I, Eric Diehl, hereby declare as follows:

1. I am over the age of 18 years and I am VP, Security Systems & Technologies of Technicolor R&D France. I have personal knowledge of all facts stated herein and all such facts are true and correct.

2. Until May 2012, I was leading the Security and Content Protection Lab of Technicolor R&D France, which has been involved in research and development efforts relating to video fingerprinting technology including, for example, those shown in Exhibit 5 to Blue Spike's December 13, 2012 brief (*see* ECF No. 16-5). More specifically, Technicolor R&D France employees—including myself—have engaged in research and development efforts relating to video fingerprinting and have designed video fingerprinting prototype programs, including a program referred to as Spider; however, all of that work occurred in Europe and none of it ever resulted in a product or service that was commercialized in the United States or elsewhere. Additionally, employees of Technicolor R&D France have published academic

articles on video fingerprinting, and demonstrated prototype video fingerprinting software in California. No employee of any Technicolor entity has ever demonstrated any video fingerprinting software in Texas. Moreover, none of the foregoing is related in any way to Technicolor SA or Technicolor USA, Inc.

3. Exhibit 5 attached to Plaintiff Blue Spike's December 13, 2012 brief (*see* ECF No. 16-5) is a fact sheet describing a video fingerprinting prototype developed by the Security & Content Protection Lab, which is a division of Technicolor R&D France. As I described above in paragraph 2, this system has never been offered for sale, sold, made, or used in the United States, or imported into the United States. Moreover, this fact sheet does not identify any video fingerprinting technology of Technicolor SA or Technicolor USA, Inc. In addition, I am listed as the contact person on the last page of this fact sheet, and I am not an employee of Technicolor SA or Technicolor USA, Inc.

4. Exhibit 6 attached to Plaintiff Blue Spike's December 13, 2012 brief (*see* ECF No. 16-6) appears to be an online article dated September 25, 2012, interviewing me about a presentation I made at the 2012 APEX Conference in California. I attended the APEX conference as an employee/representative of Technicolor R&D France. During this conference dedicated to Inflight Entertainment Systems (IFE), I presented a lecture entitled securing digital content (see Exhibit A). The first part presents a typical multi-layer approach of content protection. In the remainder of the presentation, I focus on the issues related to IFE. The section called Tool Box presented some potential solutions proposed by Technicolor. None of them uses video fingerprinting techniques. Additionally, as this article mentions, I also gave a similar presentation in Burbank California. I have never attended any trade shows in Texas on behalf of any Technicolor entity, including Technicolor SA and Technicolor USA, Inc., nor have I have

ever traveled to Texas to give any presentations on behalf of any Technicolor entity, including Technicolor SA and Technicolor USA, Inc.

5. I have reviewed the You Tube video at web address http://bit.ly/VrJ0Tp, which was cited in Blue Spike's brief (ECF No. 14 at p. 2 and p. 7, note 2). Nothing in this video refers to Technicolor SA or Technicolor USA, Inc. or any product or service of Technicolor SA or Technicolor USA, Inc. Rather, portions of this video are describing research projects similar to those referenced in Exhibit 5 (discussed above), including the Spider project that my team developed. The Spider project never made it out of research, and was never used, made, sold, offered for sale, or imported into the United States. The remaining portions of this video are describing the Genuine DVD Authentication ("GDA") concept, which is unrelated to video fingerprinting, and which is not a concept of either Technicolor SA or Technicolor USA, Inc.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Date: 21- February 2013

By: DIEHL Eric
Title: VP Security Systems & Technology

DECLARATION OF ERIC DIEHL IN SUPPORT OF DEFENDANT TECHNICOLOR SA'S REPLY BRIEF IN SUPPORT OF ITS MOTION TO DISMISS FOR LACK OF PERSONAL JURISDICTION, IMPROPER VENUE, AND INSUFFICIENT SERVICE OF PROCESS

EXHIBIT A

Securing content

DIEHL Eric

Technicolor

technicolor

Security Laboratories

apex 2012EXPO

17-20 SEPTEMBER LONG BEACH, CA USA

Agenda

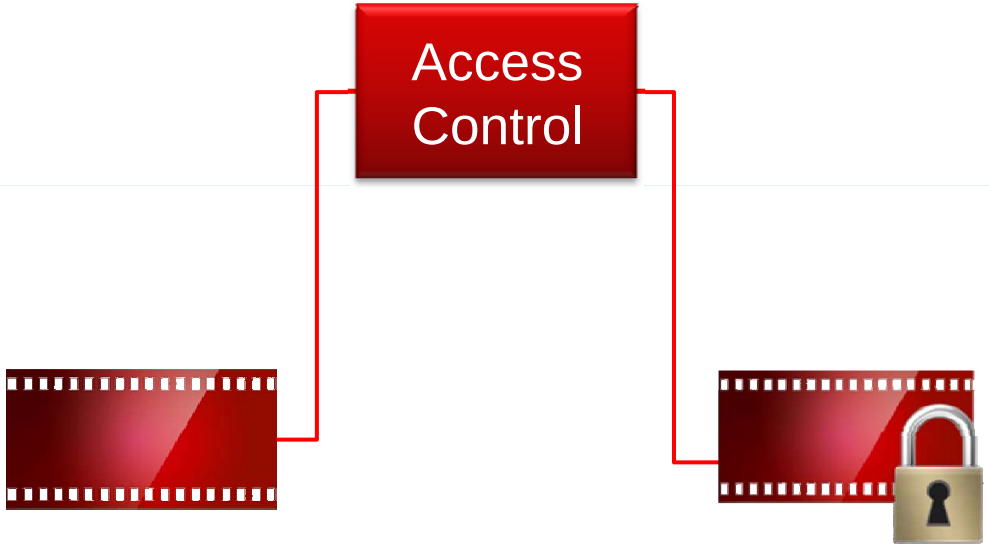
- A multi-layer approach for protecting content
- Threat analysis
- A tool box
- Some ideas for IFE

- **A multi-layer approach for protecting content**
- Threat analysis
- A tool box
- Some ideas for IFE

First Security Goal

Control access to assets

- Only authorized users should have access
- Professional premises
- Not effective against insiders



Solutions

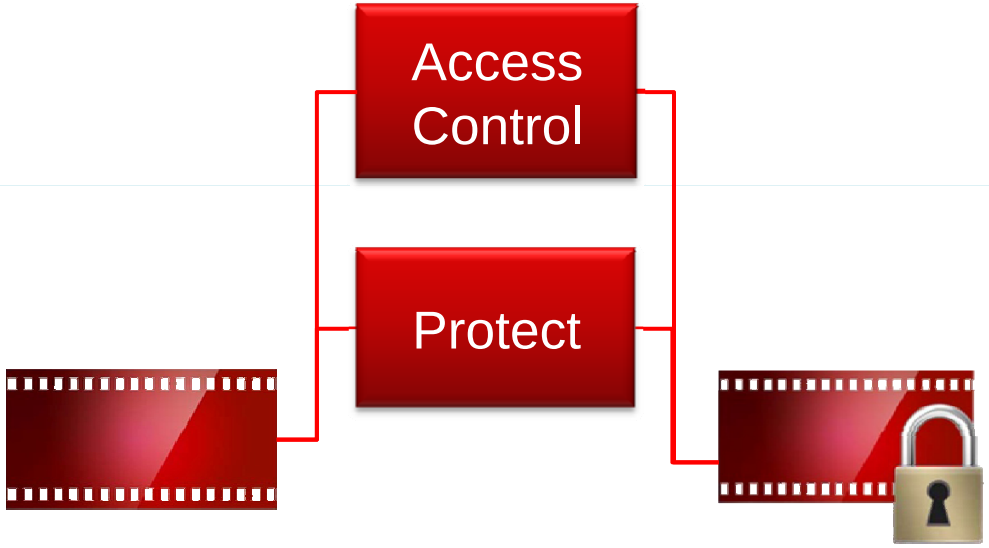
➔ Physical security

➔ IT security

Second Security Goal

Protect the assets

- Make theft useless and prevent alteration
- All along the chain
- Physical and digital domain



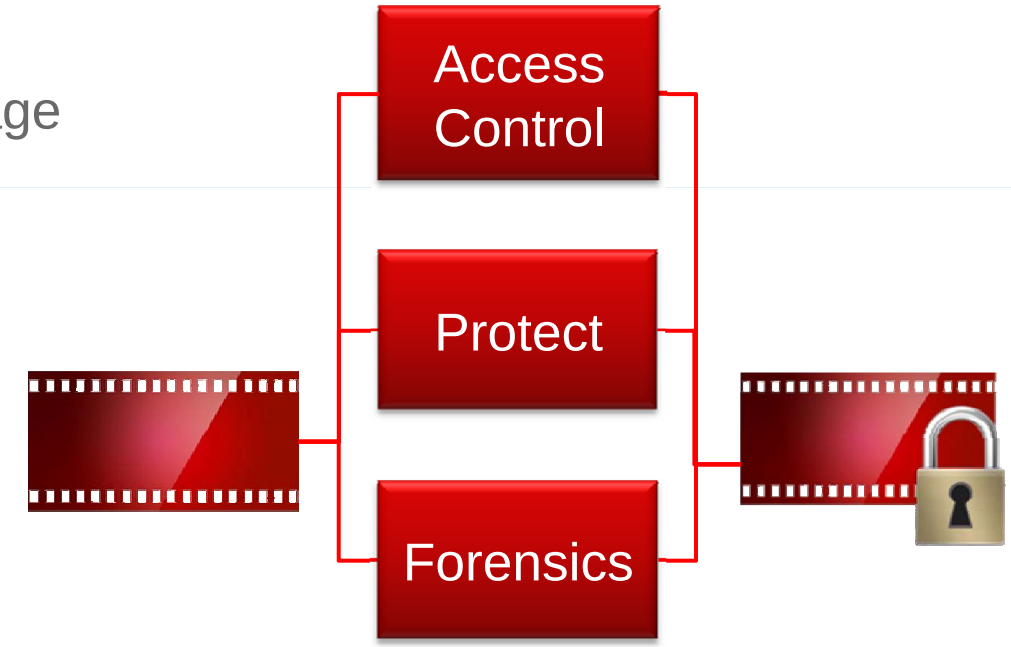
Solutions

➔ Encryption

Third Security Goal

Trace the assets

- Trace back the origin of leakage
- All along the chain
- A posteriori
  - It is too late
  - Corrective actions



Solutions

➔ Forensics watermark

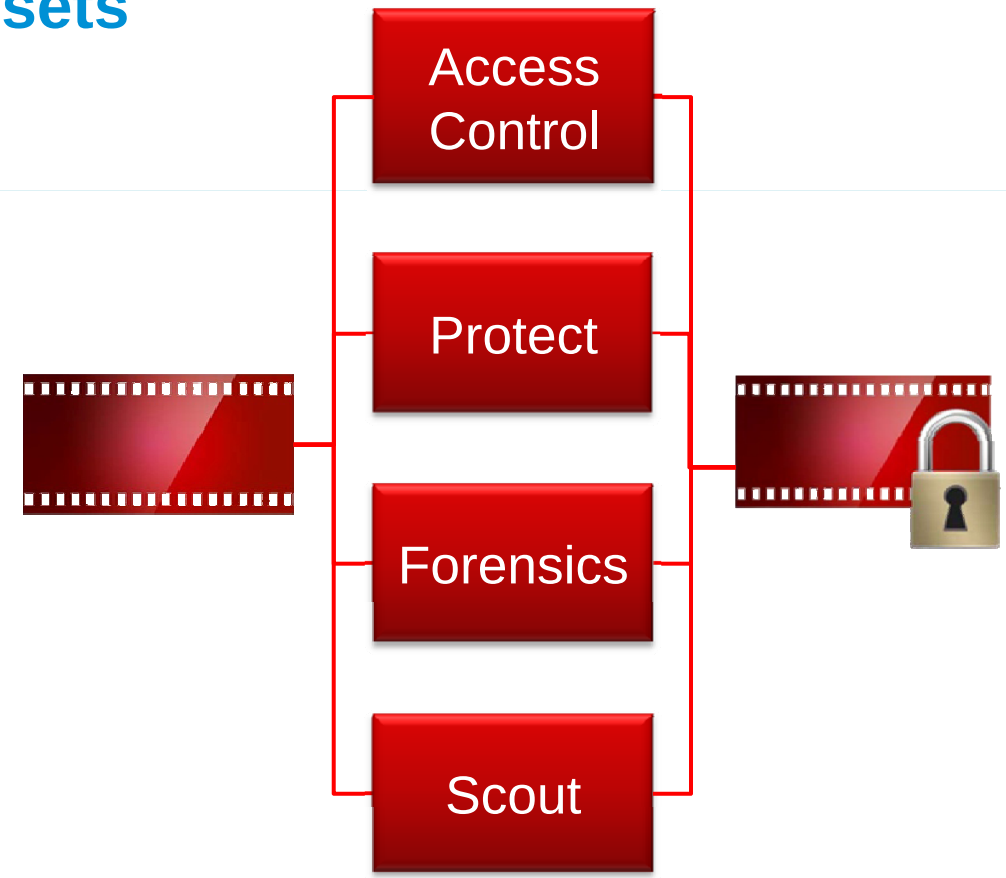
→ Video

→ Audio

Fourth Security Goal

Limit illegal use of the assets

- Spot illegal content
- Internet
- Too late



Solutions

➔ Video fingerprint

➔ Forensics detection

An example: today event

EVENT DATE: Sunday 16 Septemb
EVENT TIME: 3:30pm – 5:
LOCATION: #347
…

AUDITORIUM:
AUDITO

POWERPOINT:
studio

SECURITY:

SECURITY CON
SECURITY GUARDS
OTHER SECURITY:
etc.

EVENT DATE: **Sunday 16 September**
2:30pm – 5:30pm

SERVER: **Doremi Imb 2K, Serial**
#221377

-23B,

SERVER: Imb 2K **Serial**

SECURITY GUARDS: Four (4) Security Guards at rehearsals through end of event

OTHER SECURITY: Metal wands, **night vision goggles, NDAs for attendees**, bag and tag all phones, computers

- A multi-layer approach for protecting content
- **Threat analysis**
- A tool box
- Some ideas for IFE

Threats for IFE

Main threat

- Leakage of early content
  - During Quality Control and integration
  - After release to airline

Secondary threat

- Illegal sharing of content between carriers
- Use of content outside the agreed conditions
- Alteration/replacement of a piece of content

Security Goals for IFE

Security goals

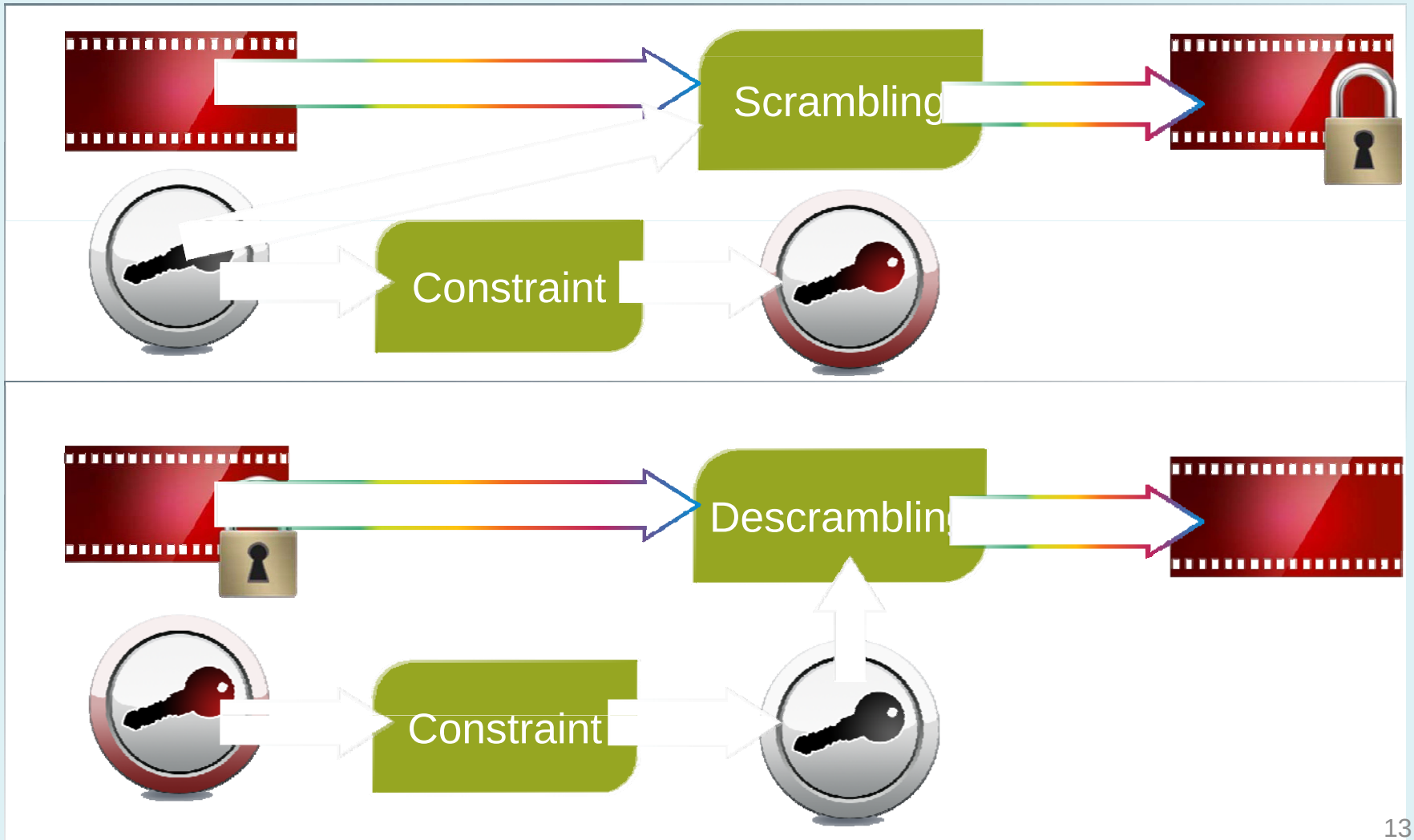
- Trace the source of leakage
  - What level of granularity?
- Control the usage of content
  - Who, where, and when

Constraints

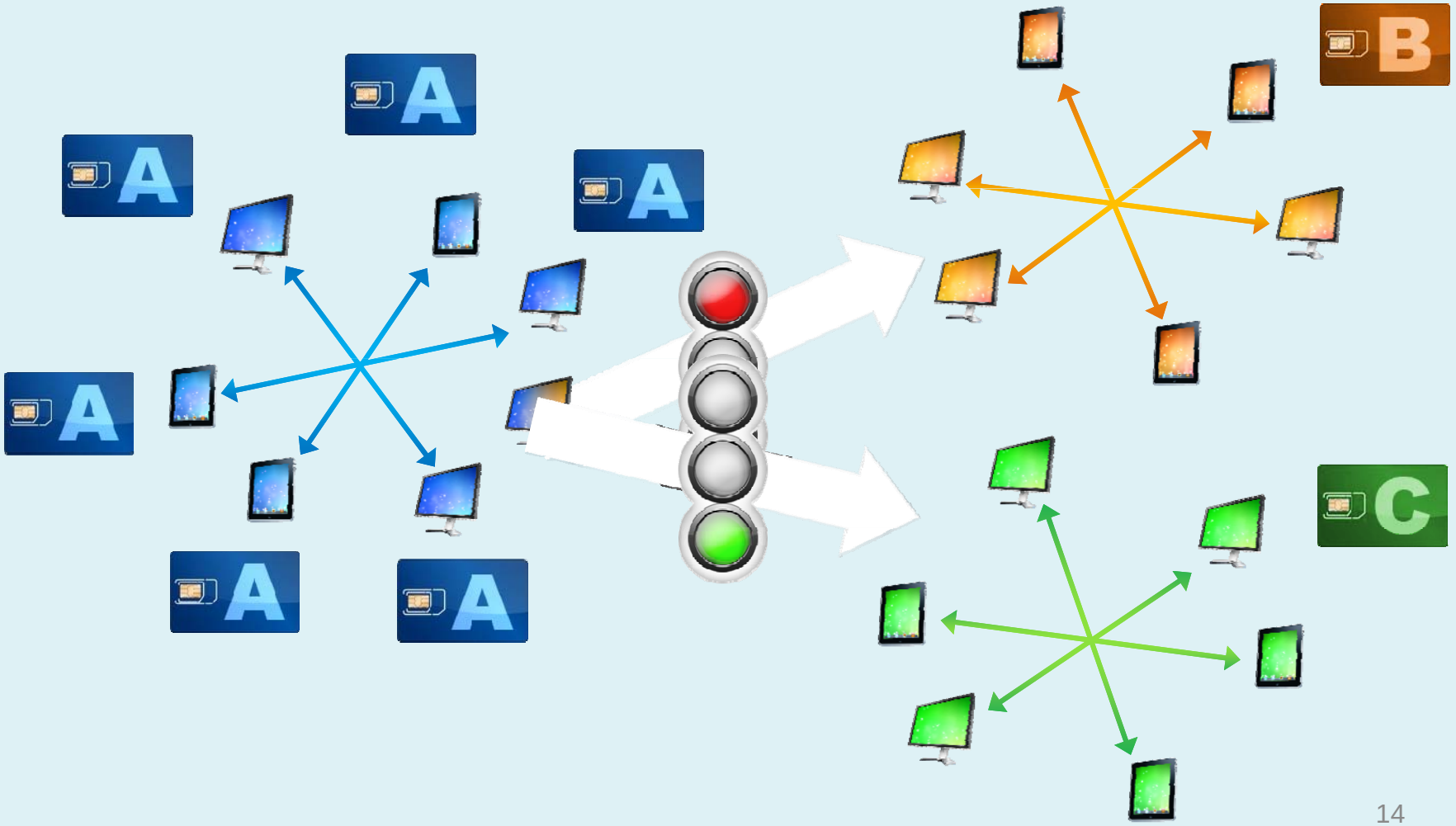
- Transparent to cabine crew and passengers
- No undue burden on logistics

- A multi-layer approach for protecting content
- Threat analysis
- **A tool box**
- Some ideas for IFE

Encryption



Domain Key Management



Watermark

Information strongly embedded in content

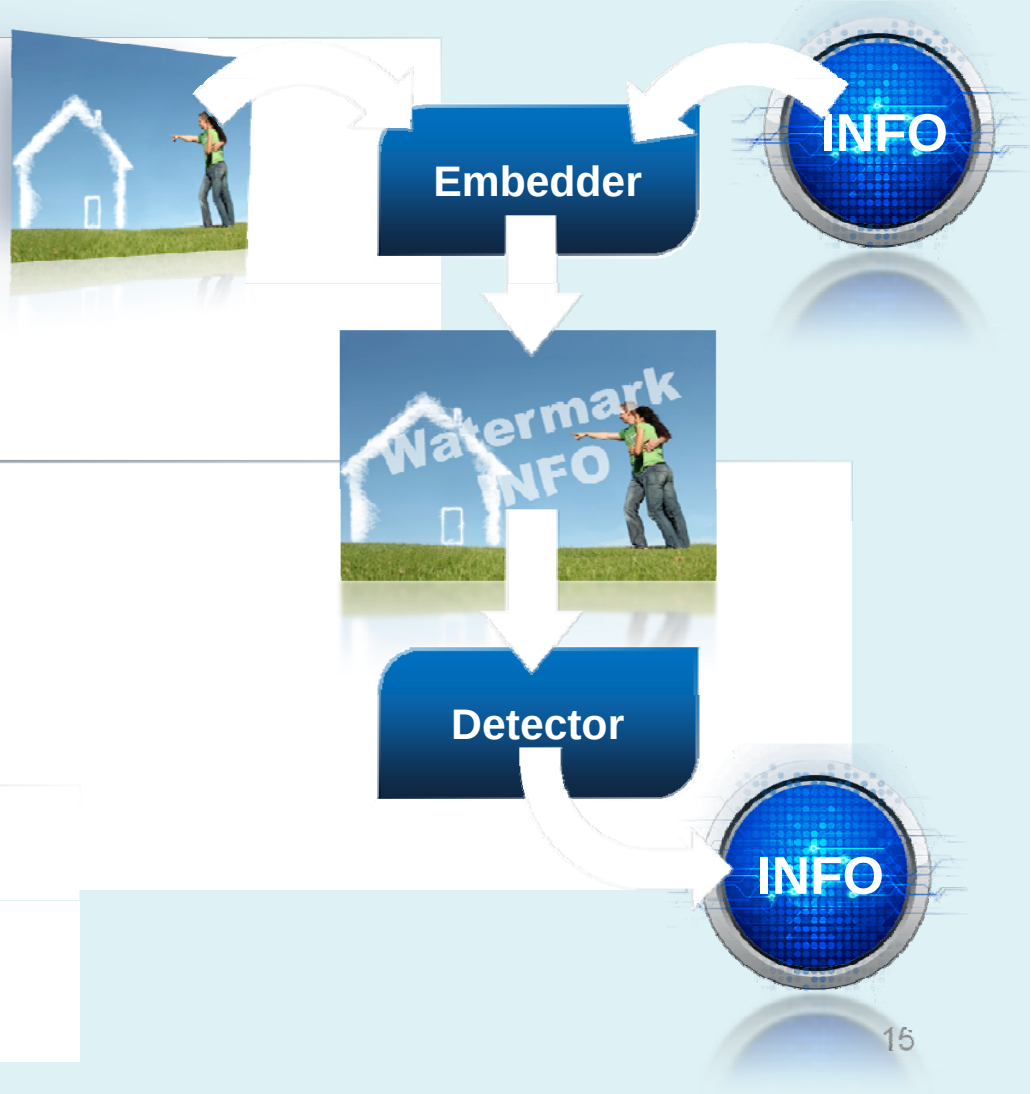
- Imperceptible
  - Audio
  - Video

Robust to « attacks »

- Voluntary
- Involuntary
  - Normal transformation

Payload

- AirLine
- Flight number



New Generation of Video Watermark

New Generation of Video Watermark

Two-step watermark

- Profiling
- Embedding

Low calculation for embedding

- Blitz fast
- Easy and cheap to implement
  - Seat box
  - Dedicated player in personal device

apex 2012 EXPO

The Art of Securing Digital Video

Security is a complex task with many pitfalls

- Ten laws
  - ➔ http://eric-diehl.com/index.php?lang=En&page=lois

Encryption is not just a good algorithm

- Robust implementation is key
  - Too easy to make loosy implementations

Security is not stronger than its weakest point

- An overall complex set of interacting defenses

Hackers are bright

- Security is a mindset

Trust and skill

apex 2012 EXPO

Technicolor Quarterly Security Newsletter

Subscribe at

- security.newsletter@technicolor.com

Past issues at

- http://eric-diehl.com/index.php?lang=En&page=news

- A multi-layer approach for protecting content
- Threat analysis
- A tool box
- **Some ideas for IFE**

Advanced System for End-to-End Security

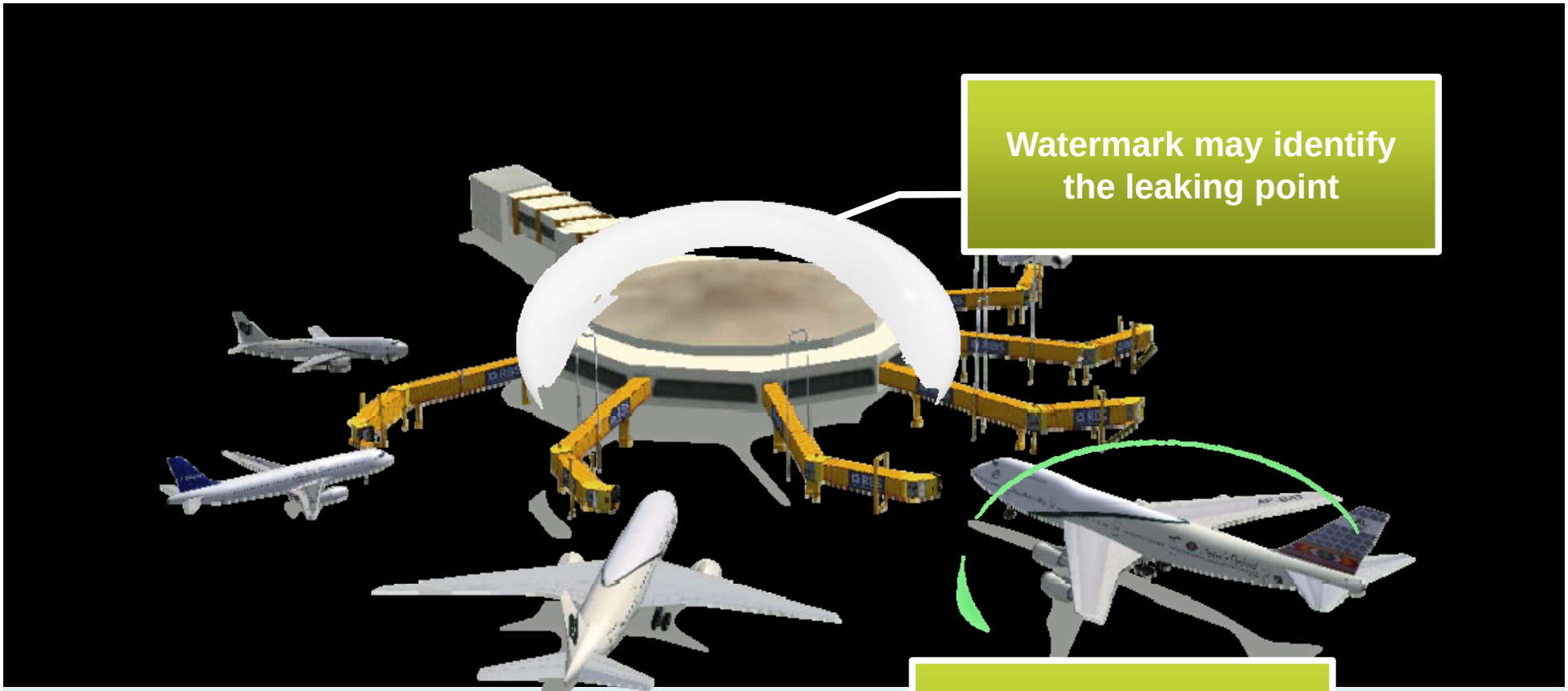
Domain based encryption

- All along the chain with isolating domains
  - QC
  - Airline Hub
  - Plane

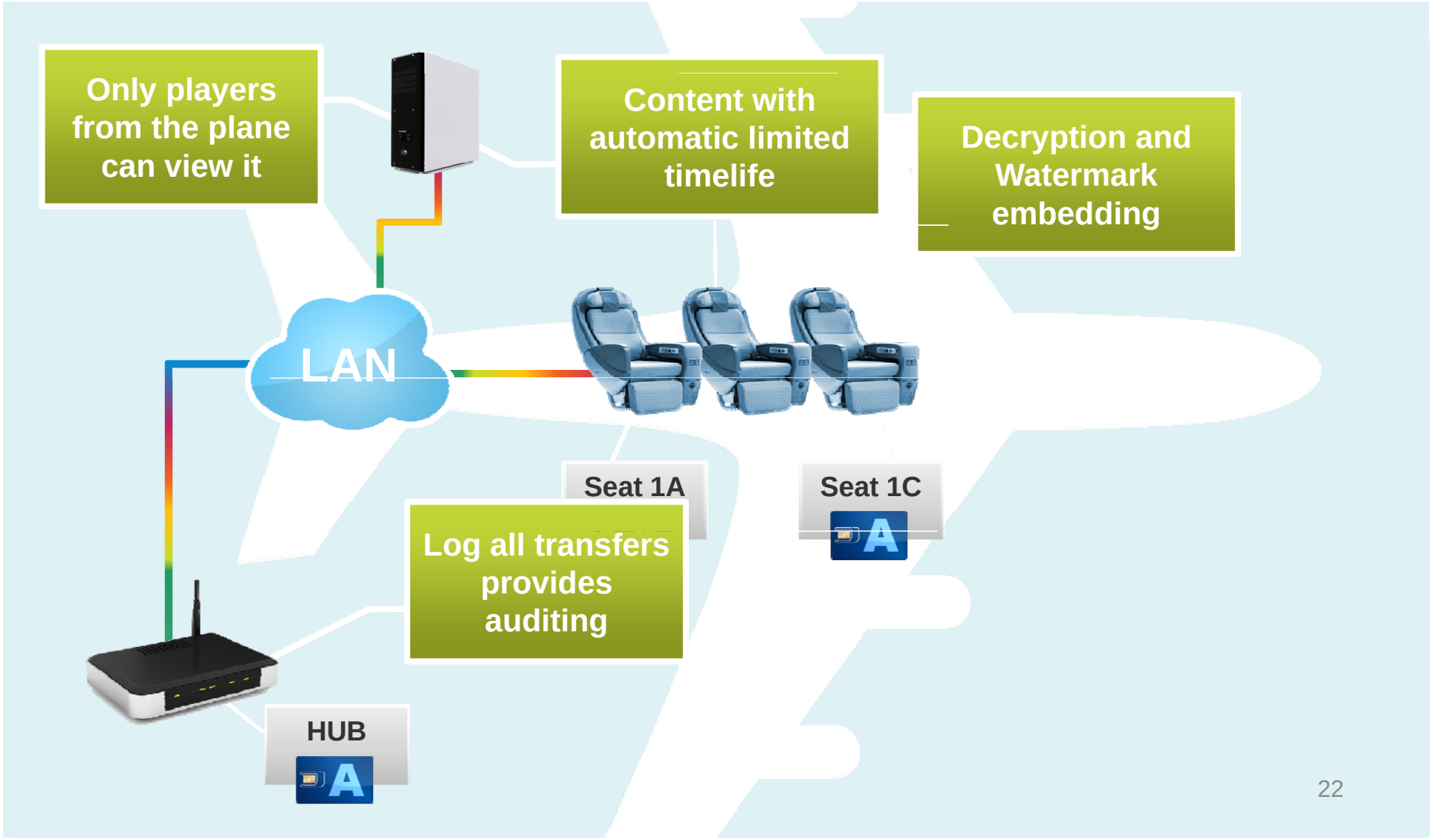
Individual watermark at rendering point

- Payload to be defined
  - Time stamp
  - Viewer ID

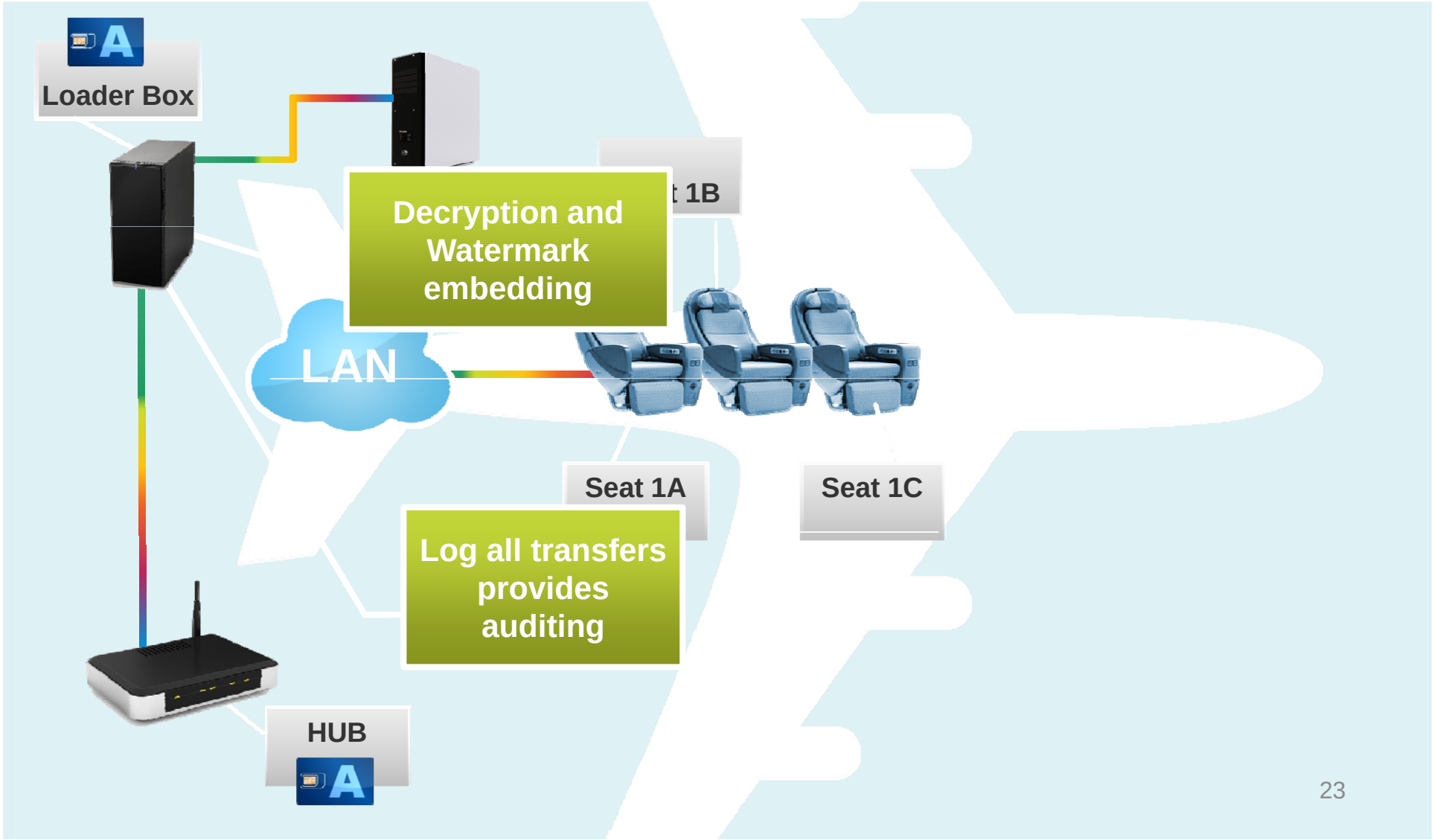
Example 1: Distribution Scheme for Flight



Example 1: Encrypted within Plane



Example 2: Clear within Plane (legacy)



technicolor

Security Laboratories

Thank you for your attention